Algèbre 2 - arithmétique et dénombrement

1 Rudiments d'arithmétique dans $\mathbb{Z}$

Définition (divisibilité)**.** *Soit $a, b \in \mathbb{Z}$. On dit que b est un **diviseur** de a s'il existe $q \in \mathbb{Z}$ tel que $a = bq$. On note alors $b \mid a$ ("b divise a"). On dit aussi que a est un **multiple** de b.*

Remarques.

- 1 *divise tous les entiers car pour tout $a \in \mathbb{Z}$, $a = 1 \times a$.*
- 0 *ne divise aucun entier à part lui-même, puisque pour tout $q \in \mathbb{Z}$, $0 \times q = 0$.*
- *Tous les entiers $b \in \mathbb{Z}$ divisent 0 car $0 = b \times 0$.*

Ex : les diviseurs positifs de 24 sont :

$$\mathcal{D}(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

Théorème (division euclidienne dans $\mathbb{Z}$)**.** *Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que :*

$$\begin{cases} a = bq + r \\ 0 \leqslant r \leqslant b - 1 \end{cases}$$

*q s'appelle le **quotient** de la division euclidienne de a par b, et r le **reste**.*

Ex : la division euclidienne de 67 par 4.

67	4
−40	16
27	
−24	
3	

quotient

STOP car $\in [\![0, 3]\!]$

67	4
27	16
3	

D'où :

$$67 = 4 \times \underbrace{16}_{\text{quotient}} + \underbrace{3}_{\text{reste}}$$

La division de 4 par 67 est immédiate :

$$4 = 67 \times \underbrace{0}_{\text{quotient}} + \underbrace{4}_{\text{reste}}$$

Remarque. *Si $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, on a l'équivalence :*

$$(b \text{ divise } a) \iff (\text{Le reste de la division euclidienne de } a \text{ par } b \text{ est } 0)$$

Cf exo 1

Définition (Nombre premier)**.** *Un entier $p \geqslant 2$ est dit **premier** si ses seuls diviseurs positifs sont 1 et lui-même.*
L'ensemble des nombres premiers est traditionnellement noté $\mathbb{P}$.

Théorème. *Tout entier $n \geqslant 1$ se décompose de manière unique sous la forme :*

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k}$$

où :

- *$p_1, \ldots, p_k$ sont des nombres premiers (distincts) ;*
- *$\alpha_1, \ldots, \alpha_k$ sont des entiers naturels non nuls.*

Démonstration. Hors programme, mais on peut donner les idées :

— existence : une récurrence forte sur n, sans difficulté, car dans l'hérédité, soit $n+1$ n'admet aucun diviseur $\geqslant 2$, et donc il est premier (et il est égal à lui-même à la puissance 1), soit il en admet, $n+1 = a \times b$, et on peut appliquer l'hypothèse de récurrence à a et b ;

— unicité : plus difficile. Pour le coup, il faut faire un peu d'arithmétique, avec le lemme de Gauss pour avoir qu'un nombre premier ne peut pas diviser un produit d'autres nombres premiers.

□

Proposition. *Il existe une infinité de nombres premiers.*

Démonstration. Raisonnons par l'absurde, et supposons qu'il existe un nombre fini de nombres premiers : $p_1, \ldots, p_n$. On pose alors :

$$m := \left(\prod_{k=1}^{n} p_k\right) + 1$$

Comme $m \geqslant 2$, m admet une décomposition du type $m = p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n}$, dans laquelle au moins l'un des α_i est supérieur à 1, ce qui signifie que p_i divise m. Or, pour chaque p_i, la définition de m, qui peut être écrite de la façon suivante :

$$m = p_i \times \left(\prod_{k \neq i} p_k\right) + 1$$

implique que le reste de la division euclidienne de m par p_i est 1.
Cela prouve qu'aucun des p_i ne divise m. **Contradiction.** □

Définitions (PGCD et PPCM)**.** *Soit $a, b \in \mathbb{Z}$, tels qu'au moins l'un des deux est non nuls.*

- *Le PGCD (plus grand commun diviseur) de a et b est le plus grand des entiers qui sont à la fois diviseurs de a et de b. Cet entier est bien défini puisque l'ensemble des diviseurs communs à a et b est non vide (il contient 1 par exemple), et majoré (par exemple par $|a|$ ou par $|b|$ si $a = 0$).*
  Le PGCD de a et b est noté $a \wedge b$, $pgcd(a, b)$, ou $PGCD(a, b)$.
- *Le PPCM (plus petit commun multiple) de a et b est le plus petit des entiers positifs qui est à la fois un multiple de a et un multiple de b. Cet entier est bien défini puisque a et b admettent toujours des multiples communs positifs (par exemple $|ab|$), et est minoré par 0.*
  Il est noté $a \vee b$, $ppcm(a, b)$ ou $PPCM(a, b)$.

Vocabulaire. *Lorsque deux entiers ont un PGCD égal à 1, ce qui signifie qu'ils n'ont aucun diviseur commun (et donc aucun nombre premier en commun dans leurs décomposition respectives), on dit qu'ils sont* ***premiers entre eux****.*

Il y a deux méthodes classiques pour calculer le PGCD de deux entiers $a, b \in \mathbb{N}^*$.

▶ **Méthode 1 : utiliser la décomposition en facteurs premiers**
Exemple pour le calcul du PGCD de 66 et 24. On les décompose :

$$66 = 2 \times 3 \times 11 = 2^1 \times 3^1 \times 11$$
$$24 = 2^3 \times 3 = 2^3 \times 3^1 \times 11^0$$

Les diviseurs positifs de 66 et 24 ne peuvent pas avoir dans leur décomposition d'autres nombres premiers que 2, 3 et 11, sans quoi ils ne divisent pas a et b. Ils sont donc nécessairement de la forme

$$d = 2^\alpha \times 3^\beta \times 11^\gamma$$

De plus :

- $\alpha \leqslant 1$, car si $\alpha > 1$, d ne divise pas 66 ;
- $\beta \leqslant 1$, sinon d ne divise ni 66 ni 24 ;
- $\gamma = 0$ sinon d ne divise pas 24.

Finalement, le plus grand diviseur que l'on peut construire est :

$$2^1 \times 3^1 \times 11^0 = \boxed{6}$$

De façon générale, si

$$a = p_1^{\alpha_1} \times \cdots \times p_n^{\alpha_n} \qquad \text{et} \qquad b = p_1^{\beta_1} \times \cdots \times p_n^{\beta_n}$$

alors

$$\mathrm{PGCD}(a,b) = p_1^{\gamma_1} \times \cdots \times p_n^{\gamma_n} \quad \text{où } \gamma_i = \min(\alpha_i, \beta_i)$$

▶ **Méthode 2 : l'algorithme d'Euclide**

Lemme. *Si $a, b \in \mathbb{N}$ sont deux entiers dont un au moins est non nul, alors $PGCD(a,b) = PGCD(b,r)$, où r est le reste de la division euclidienne de a par b.*

Démonstration. Notons $a = bq + r$ la division euclidienne de a par b. Si d est un diviseur commun de a et b ($a = da'$ et $b = db'$, alors c'est aussi un diviseur de r, car :

$$r = a - bq = da' - db'q = d(a' - db')$$

Réciproquement, si d est un diviseur commun de b et r ($b = db'$ et $r = dr'$), c'est aussi un diviseur de a car :

$$a = bq + r = db'q + dr' = d(b'q + r')$$

Conclusion : les couples (a,b) et (b,r) ont exactement les mêmes diviseurs communs, et donc en particulier le même PGCD. □

L'algorithme d'Euclide consiste à effectuer des divisions euclidiennes successives, jusqu'à obtenir 0.
Pour $a = 66$ et $b = 24$:
— division de 66 par 24 : $66 = 2 \times 24 + \boxed{18}$
— division de 24 par 18 : $24 = 1 \times 18 + \boxed{6}$
— division de 18 par 6 : $18 = 3 \times 6 + \boxed{0}$ STOP !
Par le lemme, on a :

$$\mathrm{PGCD}(66,24) = \mathrm{PGCD}(24,18) = \mathrm{PGCD}(18,6) = \mathrm{PGCD}(6,0) = \boxed{6}$$

La suite d'entiers définie par restes successifs finira toujours par valoir 0 puisqu'il s'agit d'une suite d'entiers positifs strictement décroissante.

2 Cardinal d'un ensemble fini

Définition. *On dit qu'un ensemble E est **fini** lorsqu'il contient un nombre fini d'éléments. Ce nombre s'appelle le **cardinal** de E, et est noté $Card(E)$ (ou parfois $|E|$ ou $\#E$).*

Propriétés. *Soit E un ensemble fini.*

- *Si A est une partie de E (notation : $A \subset E$), alors A est fini, et :*

$$Card(A) \leqslant Card(E)$$

- *Le complémentaire $\bar{A}$ de A dans E est fini et :*

$$Card(\bar{A}) = Card(E) - Card(A)$$

- *Si $A \subset E$, on a l'équivalence :*

$$(A = E) \iff Card(A) = Card(E)$$

- *Si A et B sont deux parties de E alors :*

$$Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B)$$

*En particulier, $Card(A \cup B) \leqslant Card(A) + Card(B)$, et il y a égalité ssi A et B sont **disjoints**, c-à-d si $A \cap B = \emptyset$.*

- *Si $A_1, \dots, A_p$ sont p parties de E, on a :* $Card(A_1 \cup \dots \cup A_p) \leqslant \sum_{k=1}^{p} Card(A_k)$

  et si les A_k sont 2 à 2 disjoints, alors : $Card(A_1 \cup \dots \cup A_p) = \sum_{k=1}^{p} Card(A_k)$.

Théorème (Cardinal d'un produit cartésien)**.**

1. *Si E et F sont deux ensembles finis, alors $E \times F$ est fini, et :*

$$Card(E \times F) = Card(E) \times Card(F)$$

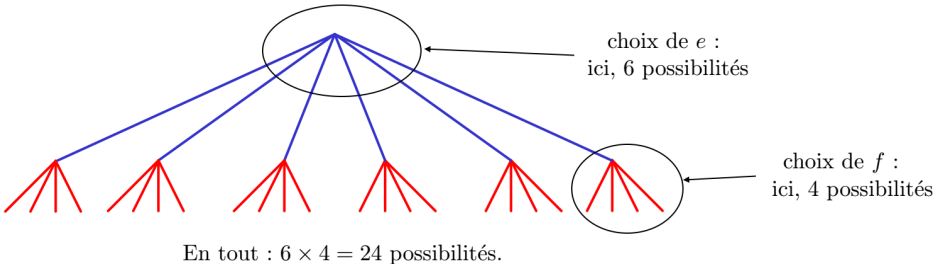
2. *Si $E_1, \dots, E_p$ sont p ensembles finis, alors $E_1 \times \dots \times E_p$ est fini, et :*

$$Card(E_1 \times \dots \times E_p) = \prod_{k=1}^{p} Card(E_k)$$

Démonstration.

1. Notons $n_E = \text{Card}(E)$ et $n_F = \text{Card}(F)$. Un élément de $E \times F$ est un couple (e, f) où $e \in E$ et $f \in F$. Une façon de construire un tel objet est la suivante :
   - on choisit e, un élément de E : n_E possibilités ;
   - **puis** on choisit $f \in F$: n_F possibilités.

   On a construit un arbre à n_E branches, dont chaque branche contient n_F sous-branche, d'où en tout $n_E \times n_F$ sous-branches.



2. Récurrence sur p, en écrivant dans l'hérédité :

$$\begin{aligned}\text{Card}(E_1 \times \dots \times E_p \times E_{p+1}) &= \text{Card}\big((E_1 \times \dots \times E_p) \times E_{p+1}\big) \\ &= \text{Card}(E_1 \times \dots \times E_p) \times \text{Card}(E_{p+1})\end{aligned}$$

□

Théorème (Cardinal de $\mathcal{P}(E)$)**.**
Si E est fini à n éléments, alors l'ensemble de ses parties (noté $\mathcal{P}(E)$) est fini, et :

$$Card(\mathcal{P}(E)) = 2^n$$

Démonstration. Notons $n = \text{Card}(E)$ et $E = \{e_1, \dots, e_n\}$. Une façon de construire une partie A de E est la suivante :

- On choisit si e_1 est dans A, ou pas : 2 possibilités.
- Puis on choisit si e_2 est dans A, ou pas : 2 possibilités.
- etc...
- Puis on choisit si e_n est dans A, ou pas : 2 possibilités.

Finalement, il y a $2 \times 2 \times \dots \times 2 = 2^n$ possibilités pour choisir A. □

3 Listes

Dans cette partie, $E = \{e_1, \dots, e_n\}$ désigne un ensemble à n éléments, et p est un entier naturel.

Définitions.

- *Une p-**liste** de E est un p-uplet d'éléments de E, c-à-d un objet de la forme $(x_1, \dots, x_p) \in E^p$. ATTENTION : l'ordre des éléments **compte**. Par ex, $(1,2,3) \neq (2,1,3)$.*
- *Une **permutation** de E est une n-liste de E où chacun des n éléments de E apparaît exactement une fois.*

Remarque : on peut aussi définir une permutation comme étant une bijection de E dans E. Les deux définitions sont équivalentes. En effet, si f est une bijection, on peut lui faire correspondre la n-liste $(f(e_1), \dots, f(e_n))$, qui est bien une permutation au sens de la 1ère définition, et cette n-liste caractérise f. (à méditer)

Théorème.

1. *Le nombre de p-listes de E est : n^p*
2. *Le nombre de p-listes d'éléments **distincts** de E est : $n(n-1)\dots(n-p+1) = \dfrac{n\,!}{(n-p)!}$*
3. *Le nombre de permutations de E est : $n\,!$*

Démonstration.

1. L'ensemble des p-listes est en fait $E \times \cdots \times E = E^p$. Leur nombre est donc $\mathrm{Card}(E)^p = n^p$.
2. Voici une façon de construire une p-liste d'éléments distincts de E :
   - On choisit le 1er élément de la liste : n possibilités.
   - Puis on choisit le 2ème : $n-1$ possiblités, car on ne peut pas reprendre le premier.
   - Puis le 3ème : $n-2$ possibilités.
   - etc...
   - Puis le p-ième : $n-(p-1)$ possibilités, car $p-1$ valeurs sont déjà prises.

   Finalement, le nombre de listes possibles est
   $$n(n-1)\cdots(n-p+1) = \frac{n(n-1)\cdots(n-p+1)\times(n-p)\cdots 2\cdot 1}{(n-p)\cdots 2\cdot 1} = \frac{n!}{(n-p)!}$$
3. Il s'agit du cas où $p = n$. On obtient donc d'après le résultat précédent : $\dfrac{n!}{(n-n)!} = n!$.

□

4 Combinaisons

Dans cette partie, $E = \{e_1, \dots, e_n\}$ désigne un ensemble à n éléments, et p est un entier naturel.

Définition. *Une p-**combinaison** de E est une partie de E à p éléments.*

*ATTENTION : il s'agit d'un ensemble donc l'ordre des éléments **ne compte pas**. Par ex, $\{1,2,3\} = \{2,1,3\}$.*

Théorème. *Le nombre de p-combinaisons est $\binom{n}{p}$.*

Démonstration. Notons $u_{n,p}$ le nombre de p-combinaisons. Pour déterminer $u_{n,p}$, on va compter de deux façons différentes le nombre de p-listes d'éléments distincts de E.

- **1ère méthode :** la construction de la liste de gauche à droite que nous avons déjà faite plus haut. On compte ainsi : $\boxed{\dfrac{n!}{(n-p)!}}$ possibilités.

▶ **2ème méthode :** on construit la liste en 2 étapes :

- On commence par choisir les p éléments que l'on mettra dans la liste, sans ordre. Il s'agit donc de choisir une partie de E à p éléments, c-à-d une p-combinaison. Le nombre de possibilités de le faire est donc $u_{n,p}$, par définition.
- Puis une fois que ces éléments $x_1, \dots, x_p$ sont choisis, on décide de leur ordre dans la liste. Il s'agit donc de choisir une permutation de ces p éléments, d'où p possibilités de le faire.

Finalement, on obtient $\boxed{u_{n,p} \times p!}$ listes possibles.

Conclusion : les deux résultats encadrés doivent être égaux. D'où

$$\frac{n!}{(n-p)!} = u_{n,p} \times p! \qquad \text{donc} \qquad u_{n,p} = \frac{n!}{p!(n-p)!} = \binom{n}{p}$$

□

Cf exo 3

5 Cardinaux et applications

Dans cette partie, $E = \{e_1, \dots, e_p\}$ et F sont deux ensembles finis de cardinaux respectifs p et n, et f désigne une application de E dans F.

Remarques.

- *Si $p > n$, c-à-d $Card(E) > Card(F)$, alors f ne peut pas être injective.*
  En effet, par l'absurde, si f est injective, alors les images $f(e_1), \dots, f(e_p)$ sont toutes distinctes, ce qui met en évidence p éléments différents de F. C'est impossible puisque le nombre d'éléments de F est strictement inférieur à p.
- *A l'inverse, si $p < n$, f ne peut pas être surjective. Les $f(e_1), \dots, f(e_p)$ sont en trop petit nombre pour prendre toutes les valeurs de F.*
- *Finalement, s'il existe une bijection entre E et F, alors $p = n$, c-à-d $Card(E) = Card(F)$.*

Théorème. *Si E et F ont **même cardinal** n, alors :*

1. *Si f est injective, elle est aussi nécessairement surjective (et donc bijective).*

   Démonstration. En effet, les images $f(e_1), \dots, f(e_n)$ prennent n valeurs distinctes, et cela dans F qui comprend justement n valeurs. Elles prennent donc **toutes** les valeurs. □

2. *Si f est surjective, elle est aussi nécessairement injective (et donc bijective).*

   Démonstration. Par l'absurde, si f n'est pas injective, alors parmi les $e_1, \dots, e_n$, deux éléments e_i et e_j ont la même image par f. Quelles que soient les images des autres e_k, le nombre de valeurs prises par f ne dépassera donc pas $n-1$. Donc au moins un des n éléments de F ne sera pas atteint par f. □

Conclusion : *lorsque $Card(E) = Card(F)$, on a les équivalences :*

$$(f \text{ injective}) \iff (f \text{ surjective}) \iff (f \text{ bijective})$$

Remarque. *Le nombre d'applications de E dans F est : $n^p = (Card(F))^{Card(E)}$, ce qui justifie d'ailleurs la notation F^E pour désigner l'ensemble des applications de E dans F.*

Démonstration. En effet, choisir une application $f : E \to F$ correspond à choisir la liste $(f(e_1), \dots, f(e_p))$ des valeurs de f, c'est-à-dire une p-liste de F, qui a n éléments. D'où n^p possibilités. □